Enhancing Cooperation in Wireless Vehicular Networks

J. Molina-Gil, P. Caballero-Gil and C. Caballero-Gil

Department of Statistics, Operations Research and Computing
University of La Laguna, 38271 La Laguna, Tenerife, Spain

Abstract. Vehicular Ad-hoc NETworks (VANETs) may be seen as a special case of mobile ad-hoc networks, featured by their high mobility and changing topology. They will become very important in our society because of their applications in traffic safety and management. Operations in VANETs rely on the cooperation of participating nodes to route data for each other. Consequently, the quality of communication in VANETs can be degraded if the number of non-cooperative vehicles is very large. As distributed networks, nodes might behave non-cooperatively for their own benefits. In order to prevent this non-cooperative behaviour from tampering packet relaying in the network, in this work we propose a self-organized and decentralized security mechanism. The system combines different techniques based on time and distance, reputation lists and acknowledgment messages. Within our proposal, privacy and integrity are protected while misbehaving and faulty nodes are detected and prevented from disrupting the network by using tools implemented with current technology. As an example of application of the proposal, its use to avoid traffic congestions is shown.

1 Introduction

A VANET is a wireless network spontaneously formed by vehicles in movement. It has no central infrastructure and presents unique challenges such as high node mobility, real-time constraints, scalability, gradual deployment and privacy. Its main goal is to improve safety, efficiency, and comfort in everyday road travel through the exchange of warning messages between vehicles. There are many possible situations where communication among vehicles could help to prevent accidents and to avoid collapses. VANET structure allows taking advantage of other services such as access to Internet and commercial advices. It would imply a high cost for operators to deploy the necessary infrastructure consisting in increasing the coverage of the network by adding antennas. However, as shown in this paper, there is no need for any expensive infrastructure if nodes cooperate.

Another important issue of VANETs is the cryptographic need of these networks, such as authentication, data integrity, privacy and confidentiality. In order to meet these requirements, various known mechanisms such as digital signatures, hash functions or MACs (Message Authentication Codes) and even the use of pseudonyms have been proposed. Nevertheless, all these tools require Certification Authorities (CAs), which are responsible for delivering public/private key pairs and certificates [1]. Some authors propose a Regional Transportation Authority, which can be a state, province, etc. [2].

Molina-Gil J., Caballero-Gil P. and Caballero-Gil C..
Enhancing Cooperation in Wireless Vehicular Networks.
DOI: 10.5220/0003583300910102
In *Proceedings of the 8th International Workshop on Security in Information Systems* (WOSIS-2011), pages 91-102
ISBN: 978-989-8425-61-4

Other authors propose a Department of Motor Vehicles [3]. However, none of these proposals are expected to be implemented in a near future.

In our work we propose the use of cooperative tools that can be implemented with current technology, such as laptops, smartphones, etc., which will be used to provide Global Positioning System (GPS) equipment and wireless networking communication. The goal of this work is to create a vehicular ad-hoc network using these technologies inside cars so that they can also be used as an emulation of the devices that will be implemented in future cars to form VANETs. Hence, real data obtained from these networks will be useful for the analysis of the operation in future VANETs.

Traffic jams are a major problem in modern societies because of the large amount of money spent in fuel, loss of user time, and especially CO2 emissions. We propose VANETs as a mechanism to prevent and reduce traffic congestion by distributing information among vehicles. An essential element when implementing these networks is the cooperation between vehicles because the self-managed exchange of messages about road conditions is vital. Therefore, this paper proposes a set of countermeasures to avoid uncooperative behavior.

This paper is organized as follows. Related works about cooperation in VANETs are summarized in Section 2. We describe the background in Section 3 and introduce our approach in Section 4. Section 5 provides a detailed description of the system and in Section 6 and Section 7 the proposal is analysed. Finally, conclusions are included in Section 8.

2 Related Work

In order to bring VANETs to their full potential, appropriate schemes to stimulate cooperation need to be developed according to the specific properties and potential applications of VANETs. VANET as a distributed and unbounded system can work properly only if vehicles cooperate in transmitting and forwarding packets. The resulting ad-hoc network offers several benefits but requires the mobile nodes to collaborate in forwarding packets as described for ad-hoc networks in [4]. It is reasonable to assume that each node has the goal to maximize its own benefit by enjoying network services and at the same time by minimizing its contribution. It is clear that a node must be encouraged in some way to relay information for the benefit of other nodes.

Some authors have made first approaches to the topic of cooperation in VANETs [5] [6] [7] [8] [9] proposes a flocking scheme for a group of vehicles, which focuses on their decentralized coordination such that they can cooperate. Another good example of VANET application that requires cooperation is described in [10], which proposes a framework for commercial ad dissemination in VANETs where possible non-cooperative nodes are considered.

Related to the proposal here described, Buttyan and Hubaux proposed in [11] and [12] the use of virtual credit in incentive schemes to stimulate packet forwarding in mobile ad-hoc networks. Also, Li et al. discussed some unique characteristics of incentive schemes for VANETs in [13] and proposed a receipt counting reward scheme that focuses on the incentive for spraying. However, the receipt counting scheme proposed

there has an overspending problem. Based on the specific characteristics of VANETs, a more comprehensive weighted rewarding method was proposed in [14].

A malicious attacker can cause the VANET to be broken into pieces so that the network cannot provide services such as route establishment and packet forwarding to legitimate users. In this sense, the behaviour of selfish nodes can cause a passive denial-of-service. [15] discusses some of the main security threats and attacks that can be exploited in VANETs. This paper is mainly focused on the design of packet forwarding enforcement schemes.

3 Background

At the beginning, self-managed VANETs will run with a small group of devices. These devices must have some basic mechanisms to be able to cooperate. If a device detects traffic congestion, it must notify its neighbours about it. This provides an augmented reality of what is happening on the road, what will allow other users outside the congestion zone to make decisions in time to avoid accidents and traffic jams, for example by finding an alternative route. Nodes that can check such information are responsible for determining the authenticity of the messages and reporting detected forgeries. If this happens, fake nodes will not be authenticated by anynode in the network and will be unable to get any profit from the received information. The whole process will be automatic and transparent to the network user so that there is a responsible module for detecting false or altered information. To achieve it, the forwarding messages must be signed to enable nodes to determine which is the node that presents a bad behaviour, but without revealing its real identity. In order to do it, pseudonyms will be used [16]. In addition, hash functions are used as a mechanism to determine whether the content of the message was altered during its transmission or not.

When developing the cooperation mechanism, different problems must be taken into account to make it possible that the system works properly. Moreover, as discussed above, it is required that users cooperate by relaying packets to their neighbouring nodes. Therefore, the possibility that legitimate nodes act passively only receiving information from the network should be avoided. Such a user would benefit from getting information from the network but without participating in the relay to its neighbour nodes. This would damage the network passively, by degrading its performance and threatening the connectivity. Consequently, we need a module to determine whether nodes cooperate in the network. There exists another possible attack consisting in relaying packets to overload the network. In this case, nodes would cooperate in the attack by contributing to disseminate information that is useless or repeated. Tools to avoid such attacks and their operation will be detailed below.

4 System Design

The basic idea of this work is that VANETs will allow detecting traffic jams through the automatic exchange of reports about them. This will be done thanks to the information provided by GPS because with GPS software it is possible to know the speed at which nodes are moving and the maximum speed allowed in each lane. Given this, if a vehicle

is travelling at a speed below the minimum, it is probably due to that there is congestion on that road. In this case a packet will be automatically generated to warn users about the traffic problem. This design is based on a store-and-forward routing model [13]. In a typical packet forwarding process in VANETs, vehicles encounter one another at different times, and packets are opportunistically forwarded. If an intermediate vehicle stores a packet for a fixed time or actively sprays the packet to other vehicles, the packet will be more likely to reach a greater number of vehicles.

Such as it is common when GPS is used, the user may have set the destination and the criterion that the GPS must use to find the route. This might be the shortest route, quickest route, a given time of arrival, etc. Thanks to our design, for example a GPS that has calculated as optimal route the one that crosses a highway at 80 km/h can change the selected route if it receives that the current average speed of that road is now 20 km/h due to a traffic jam.

4.1 Cooperation

A bad behaviour of a vehicle within a self-managed network can consist in:

- Inserting in the network false packets with spoofed content on the state of the road or inserting many times the same packet in search of a Denegation of Service (DoS).
- Not cooperating in relaying packets of its neighbour nodes so that it benefits from the network without cooperating in its operation.

Detection of attackers should be automatic and transparent to the user. Hence, in order to detect them, the packet must contain information about management. Thus, the packets will include the following information:

- GPS coordinates and movement direction.
- Vehicle speed.
- TimeStamp.
- Next Via.

The GPS coordinates will help in two ways. On the one hand, combined with the movement direction, they will provide information about the places where the packet was generated and where the problem is located. On the other hand, they will allow discarding packets beyond a certain range. In most cases, information generated at a certain location in a VANET is not interesting out of a radius distance. A packet can be generated in coordinates (X,Y) and certain range of interest for this packet can be defined within a radius R. In this way, the packet will not be broadcast when it reaches R and will be discarded after certain time later than the timestamp. The particular size of the radio of these zones is fixed by the source node, according to the type of road.

Vehicle speed will allow making decisions and altering the route to reach the destination. One parameter that uses a GPS device to detect the fastest or shortest route to the destination is the sum of all speeds in the used via. In this sense, our system can detect whether there is a traffic jam in a specific highway, and provide the speed at which vehicles move on it. With this information, the GPS device will be able to make calculations to determine if going through the traffic jam will take less time than modifying

the route. Otherwise it may propose a new way to reach the destination in the shortest time possible. The timestamp allows determining whether the received information is new or old. This makes possible to have updated information about the road all the time. Finally, the information about the next via let us know whether the traffic jam is across the entire highway or only in a given road of the highway.

4.2 Detecting Misbehaviour

In order to provide real-time and trustful information, each vehicle must have a list where it stores information on those vehicles that have reported misbehaviour. This list is maintained by each node and is modified during the interaction with other vehicles. It can be updated whenever it detects misbehaviour of a vehicle that forges a message that does not correspond to its real environment information. It can be also updated during the exchange of packets between two vehicles, because besides the key store exchange, they swap their lists. Thus, legitimate nodes in the network will have always an updated list so that they will not send information to nodes that have not worked within the network. Each record in this list will contain the misbehaving vehicles' pseudonyms, which will allow determining who they are when they meet. The date of a bad behaviour is used to keep the list updated by deleting old records. Another field with the signature of the node who presented the complaint is also stored, which allows avoiding a false allegations.

The next paragraphs explain how to detect bad behaviour from the information contained in the packets:

GPS Coordinates. If a vehicle A provides information about dense traffic in a road where another vehicle B is driving at an appropriate speed, the vehicle B can report that A is introducing false information. Moreover, if a vehicle is sending a packet of information outside the fix radius R, this can be reported as a DoS attempt.

Speed. If a vehicle sends information about a traffic jam in certain coordinates where the same vehicle is circulating at a high speed, this can be considered a fraud. However, if the next via in its route is nearby, this would be an exception. This circumstance will be detailed in the next section.

TimeStamp. If a vehicle is transmitting information with an expired TimeStamp, this is considered a DoS attempt.

4.3 Flexibility and Robustness

A good detection mechanism for cooperation must have two characteristics: flexibility and robustness. With regard to flexibility, note that a hardware malfunction can make the device sends messages with an incorrect or expired timestamp. Therefore we should not be too strict and allow nodes to recover from this problem. Moreover, it would be unfair to prevent the access of misbehaving nodes to the network forever after a bad behaviour. In order to solve this problem, nodes have two possibilities:

1. To get a new key pair and a pseudonym from a legitimate node belonging to the network. When a node has been marked as an attacker node, it will be isolated from the network and will not receive any traffic information. In case of malfunction, a

node can request a new key pair from a legitimate network node. Before the node receives them, it must explain the situation to the legitimate node that will provide the new key pair if it thinks it is appropriate.
2. To check whether the records in the node's lists are old enough, and delete them. The nodes will remain in the selfish node list for a period of time that will depend on the security degree and the network size. Once this period expires the node will be removed from the list and will be able to re-join the network with these credentials. Another way to remove the nodes from this list is to detect that this node has a new credential, which will mean that a legitimate network node trusts him.

The robustness of the proposed mechanism ensures that the information that reaches any nodes is true, which avoids that nodes can impersonate other nodes by sending fake packets on their behalf. To ensure this, each intermediate vehicle must be able to determine whether the information generated by the source node has not been altered. In this case, the source node computes a hash function of the packet signed with its private key and sends its public key. Thus, if the information is altered, the intermediate node will be able to detect it. Furthermore, thanks to these detection mechanisms, selfish nodes can be isolated from the network, which ensures that the nodes involved in the network are reliable and so the information they send.

4.4 Keys

During the network construction, each user must get a public/private key pair in a decentralized way. In order to achieve this goal, each new node will perform a key exchange with one or more reliable nodes in the network. Additionally, a pseudonym will be given to each new node so that it will be associated with its cooperative or selfish behaviour but without revealing its identity. This alias will be created by an automatic generator from its public key, which prevents the existence of two identical pseudonyms and the possibility of generating a false pseudonym and masquerade to be another vehicle.

Furthermore, each network node has a key store that contains other nodes' public keys signed by reliable users of the network. When two nodes meet and want to communicate with each other, their public keys are exchanged. Each public key will be looked up at the key store, and if there is no coincidence, both nodes exchange their stores. Thus, any node will try to find a common path in the resulting web of trust. Otherwise it is impossible that the nodes are authenticated and can not trust one another. This may mean that one of them has had a bad behaviour within the network. It is possible that the probability of collision at the beginning of the network is small, so low security levels will have to be defined in this sense. When the network reaches an enough size, and taking into account the small world experiment, these levels may rise.

Whenever two nodes meet in the network, they exchange their key stores, which allow them to update the information about the network. The experiments associated with the "six degrees of separation" [17] are based on the idea that if a person is one step away from each person they know and two steps away from each person who is known by one of the people they know, then everyone is at most six steps away from any other person on Earth. This idea is used in our work in two important aspects. First, according to the principle of "six degrees of separation", the probability to find

a common chain between two key stores is high so this is useful to find a match in the key stores of two nodes who do not know each other. Secondly, we will compute the probability that two nodes meet twice, which will be useful to describe our proposal.

5 Operating Mode

A vital aspect for the operation of the network is that nodes cooperate in relaying packets of their neighbouring nodes. To meet this need, we propose the use of the so-called Individual Reputation List (IRL), which is not shared with any other vehicle in the network. It allows the node to store information about cooperation got from the different nodes it meets during its life on the network. This list stores information about the direct experience of a node with other nodes of the network, so it is totally reliable for the node. Hence, thanks to the IRL the node can make decisions on whether to cooperate or not with other nodes according to the information contained in the list. In order to update such a list, an ACKnowledgment (ACK) message must be received by each node that had sent a packet. If a node A has some traffic information, before providing it to B, it asks it about B's cooperation in the network. The node B answers by providing the last ACK it has received. If the date of such ACK exceeds a limit m defined by the protocol in terms of the network size, the node A does not retransmit the packet. Thus, the nodes are motivated to cooperate in order to upgrade their ACKs. In order to avoid a possible selfish behaviour in the sending of the ACKs, a split of sent packets is introduced in the protocol. Figure 1 shows in more detail this operation.

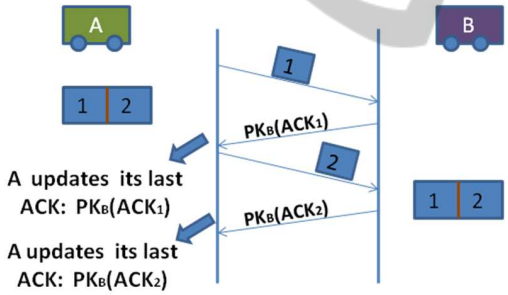

Fig. 1. Sending packets and receipt confirmations.

One node A, who wants to send a packet to B, splits it into two parts in order to ensure that node A receives at least an ACK as proof that it is cooperating before B receives the complete information. When B receives the first part of the packet, it sends an ACK signed by B, PKB(ACK). Then, A sends to B the second part of the information so that B can recover the content of the packet. Finally, B sends the second ACK to node A.

If some of these nodes decide not to relay all necessary packets for the exchange they are introduced in the IRL of the other node. This would happen if for example A does not send the second part of the packet after B has sent ACK1, or if B does not send any of the corresponding ACKs. Figure 2 shows the flowchart corresponding to the pro-

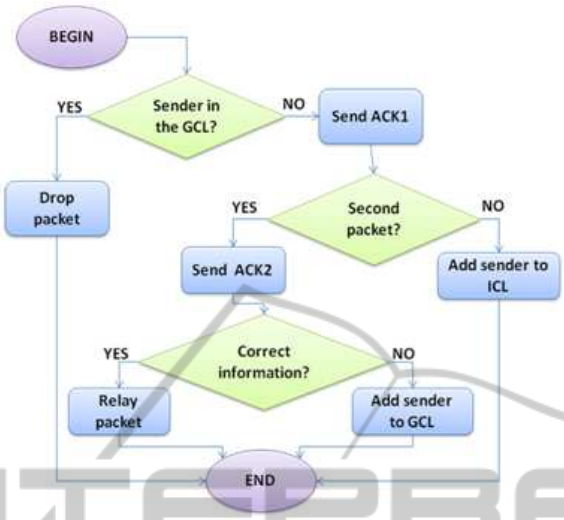

Fig. 2. Sender flowchart.

cedure when a node sends a packet while Figure 3 shows the flowchart corresponding to the process when a node that receives a packet.

According to the IRL, the nodes have an individual vision of the network. However, nodes can also have a general vision about the network through another list called General Reputation List (GRL) containing revoked pseudonyms corresponding to vehicles that had a bad behaviour within the network. In the absence of a central authority, certificate revocation must be done through cooperation and the repositories must be updated through the exchange of the GRLs among neighbouring nodes. This list can be seen as a summary of the IRL of all network nodes and therefore it provides a network overview. Its update is done each time the lists are exchanged between nodes. Thus, if a vehicle has useful information about the state of the road and finds another node that is within its GRL, it could decide not to provide it with such information. Thanks to this procedure, nodes reject selfish behaviour within the network. Moreover, if a node receives a packet from someone who is in its GRL, it discards the packet so that the misbehaving node is not able to continue attacking the network. The update process of these lists must be efficient and based on a fast search algorithm. Table 1 shows four possible fields of the records in this list. The coordinate's field is proposed as a solution to some problems of this method, which are listed in the next section.

Table 1. Fields of the GRL.

Selfish node's pseudonym	Date	Complainant node's pseudonym	Coordinates (X,Y)

6 Analysis of the Proposal

During the analysis of the proposed protocol, we realized that there exists the possibility that a vehicle has detected a traffic jam in a road where another vehicle is travelling at an appropriate speed within the same road. This could be a common situation where the left lane works properly but there is a traffic jam in a deceleration lane on the right corresponding for example to an exit to a city. In this case, besides the path and direction of traffic jams, the lanes have to be determined.

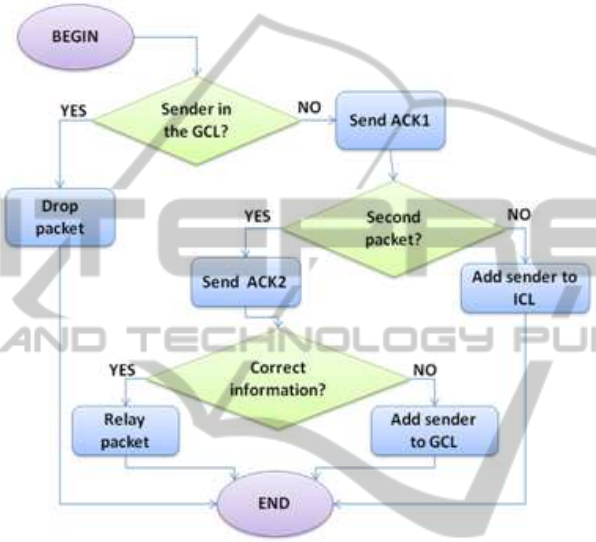

Fig. 3. Receiver flowchart.

Another possible special situation would appear when too many vehicles try to profit from the network without participating in it. The cooperation mechanism described above can solve this problem. While the system cannot ensure 100% participation of the nodes in the network, it can ensure that at some point, selfish nodes try to avoid being isolated from the network and so participate in it.

As discussed above, nodes exchange their GRLs. This implies that a node can try to attack other nodes by inserting false records in its list. Therefore we must define a criterion for determining whether a node must be isolated or not according to its appearance in the GRLs. On the one hand, a minimum number of complaints could be defined before marking a node as selfish. That is to say, if certain number of nodes agrees that a particular node is selfish, we determine that it is probably true. On the other hand, at least two of these complaints should have different coordinates (X,Y) in order to avoid specific problems detailed below. In order to choose the minimum number of complaints about the same node that must be recorded before marking it like a selfish node; a possible solution would be to set this parameter as a function of the network size. According to the small world experiment it is not difficult to find more than one coincidence. Therefore, the larger the network, the greater this number must be.

Another unusual situation appears when a vehicle is stopped on the roadway due to

an accident, car malfunction or even a phone conversation. In any of those situations, the automatic mechanism detects a vehicle at 0 km/h on a road and sends a warning about a traffic jam that does not exist. One option to solve this problem would be to revoke the car, which then should ask for a new key pair after explaining what has happened. Another possible solution would be to use the above idea and only revoke a node having a record of misconduct in more than one place from more than one node. Finally, another analyzed problem comes from the use of ACK as a cooperative mechanism. New nodes that have not participated in any packet retransmission have no ACK to receive packets from the network. One solution would be that the authenticator node gives an ACK to them. Another option would be to wait till the new nodes generate own packets of information, and after sharing them with other cars, they get an ACK and are able to participate in the network. The best option will be determined during the practical implementation of the proposal, depending on the specific conditions.

7 Simulations

Both the feasibility and effectiveness of the proposal are shown through several simulations. In particular, we used NS-2 and SUMO taking as starting point the simulations analyzed in [18]. We simulated the IRL and GRL mechanisms in a random environment to see its effects on network and cooperation performance. In order to make a study of the proposal, several VANETs simulations have been implemented. This section presents the details and results of these simulations. The aim of our proposal is to detemine and isolate from the network all malicious nodes. An interesting simulation is to determine the time required for all network nodes know which nodes are malicious in order to isolate them and prevent communications with them. The first simulation consists of a set of 100 nodes that make communications between them in a totally random way. Each simulation was performed 100 times for different percentages of malicious nodes, the graph shows the average results. If a node makes a connection to a malicious node it will be include in its IRL. However,if it connects to a node that is not malicious, simply they make an exchange of their GRL. We have set a minimum of 3 different complaints on the same node before determining that it is malicious. Figure 4 shows the time required for all nodes to determine who are the malicious nodes. As we can seen, as the number of malicious nodes increases, the time to detect them dereases. This is because there is a greater probability of encountering a malicious node and therefore the number of complaints on the nodes increases. Therefore, the mechanism works better as the number of malicious nodes increases. So we conclude that nodes will cooperate to not become isolated from the network.

Figure 4 shows that where more time is needed by the method, is on networks with 15 to 20 malicious nodes. So we took this value and we have varied the number of nodes in the network from 100 to 1000 nodes. The target is to determine how influence the number of nodes that form the network in the time needed to isolate malicious nodes from the network. In this case the results are the average of 100 simulations for the different network sizes. As shown Figure 5 the time to alert all nodes increases with the increase of the network size. However, the results shown that it is possible to isolate the malicious nodes in the network, in a reasonable time and independently the network

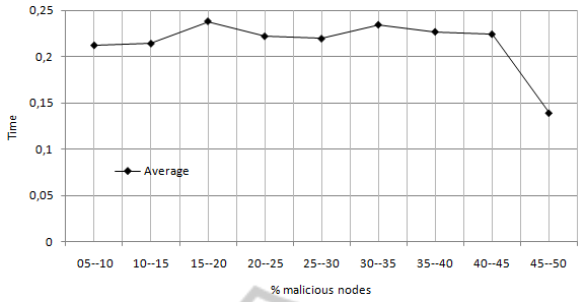

Fig. 4. Average time for warning vs. malicious nodes.

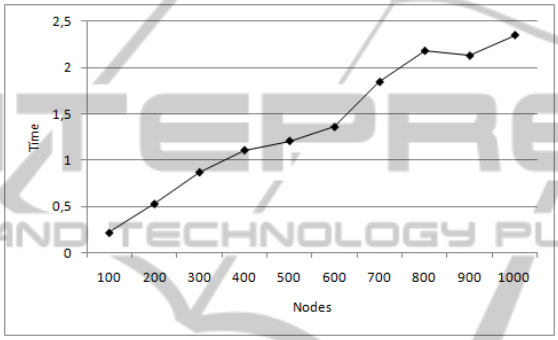

Fig. 5. Average time for warning vs. network size.

size. Therefore we can conclude that the cooperative system using reputation works properly for our proposed VANET.

8 Conclusions

This paper proposes several cooperation tools that provide a new vision of a VANET in which there is no need for any centralized authority. Thus, the aim of this work is to propose a self-managed data network that can be formed using existing technology so that nodes can receive and send information about traffic through their devices. This would allow addressing most security weaknesses of this type of networks and studying possible solutions at no cost, simply through the cooperation of users who have implemented the proposed schemes in their devices. In particular two reputation lists and acknowledgment messages as well as different mechanisms based on parameters such as time and distance have been here proposed to allow nodes to automatically detect misbehaviours. In practical simulations the proposal has shown to be useful to avoid traffic congestions.

Acknowledgements

Research supported by the Ministerio Español de Educación y Ciencia and the Europe-

an FEDER Fund under TIN2008-02236/TSI Project, and by the Agencia Canaria de Investigación, Innovación y Sociedad de la Información under PI2007/005 Project.

References

1. M. Raya, P. Papadimitratos, I. A. D. J. e.a.: Eviction of misbehaving and faulty nodes in vehicular networks. In: IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks, IEEE (2007)
2. J. Sun, Y. F.: A defense technique against misbehavior in vanets based on threshold authentication. In: IEEE MILCOM, IEEE (2008)
3. F. Li, J. W.: An innovative incentive scheme in vehicular networks. In: IEEE International Conference on Communications (ICC), IEEE (2009)
4. N. Ben Salem, L. Buttyan, J. P. H. M. J.: Node cooperation in hybrid ad hoc networks. In: IEEE Transactions on Mobile Computing (TMC), IEEE (2006)
5. F. Dotzer, L. Fischer, P. M.: Vars: A vehicle ad-hoc network reputation system. In: Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks., IEEE (2005)
6. E. Fonseca, A. F.: A survey of existing approaches for secure ad hoc routing and their applicability to vanets. In: Technical Report NLE-PR-2006-19. (2006)
7. Z. Wang, C.C.: Countermeasure uncooperative behaviors with dynamic trust-token in vanets. In: IEEE International Conference on Communications, IEEE (2007)
8. Z. Wang, C. C.: Cooperation enhancement for message transmission in vanets. In: Wireless Personal Communications: An International Journal. (2007)
9. N. Xiong, A. V. Vasilakos, L. Y. W. P. Y. Z. Y. L.: A resilient and scalable flocking scheme in autonomous vehicular networks. In: Mobile Networks and Applications, Springer (2010)
10. S.-B. Lee, G. Pan, J. S. P. M. G. S. L.: Secure incentives for commercial ad dissemination in vehicular networks. In: 8th ACM international symposium on Mobile ad hoc networking and computing. (2007)
11. L. Buttyan, J. P. H.: Stimulating cooperation in self- organizing mobile ad hoc networks. In: ACM/Kluwer Mobile Networks and Applications (MONET), MONET (2003)
12. L. Buttyan, J. P. H.: Security and cooperation in wireless networks. In: Cambridge Univ. Press, Cambridge Univ. Press (2008)
13. F. Li, J. W.: A winning-probability-based incentive scheme in vehicular networks. In: Proc. of IEEE International Conference on Network Protocols, (ICNP), IEEE (2008)
14. C. Hernández-Goya, P. Caballero-Gil, J. M. G. C. C. G.: Cooperation enforcement schemes in vehicular ad-hoc networks. In: Lecture Notes in Computer Science, Eurocast (2009)
15. J.T. Isaac, S. Zeadally, J. C.: Security attacks and solutions for vehicular ad hoc networks. In: IET Commun., IET Commun. 4 (2010)
16. L. Buttyan, T. Holczer, I. V.: On the effectiveness of changing pseudonyms to provide location privacy in vanets. In: Proceedings of the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks, Springer (2007)
17. M. Newman, A-L Barabsi, D. J. W.: The Structure and Dynamics of Networks. 1st edn. Princeton University Press, U.S.A. (2006)
18. P. Caballero-Gil, C. Caballero-Gil, J. M. G. A. Q. A.: A simulation study of new security schemes in mobile ad-hoc networks. In: Lecture Notes in Computer Science, Eurocast (2007)